UNIVERSITY OF OULU
TIETO- JA SÄHKÖTEKNIIKAN TIEDEKUNTA

Tatu Laakso
Akseli Tyvelä

Modernin IoT-laitteen tietoturvaongelmat ja -ratkaisut

Kandidaatintyö
Tietotekniikan tutkinto-ohjelma
Helmikuu 2019

Tyvelä A, Laakso T. (2019) Modernin IoT-laitteetn tietoturvaongelmat ja -ratkaisut. Oulun yliopisto, tietotekniikan tutkinto-ohjelma. Kandidaatintyö, 36 s.

TIIVISTELMÄ

Tässä kandidaatintyössä perehdytään IoT-laitteissa piileviin tietoturvaongelmiin ja niiden ratkaisuihin. Työssä käydään läpi yleisimmät IoT-laitteita kohtaavat haavoittuvuudet, niihin johtaneet syyt sekä niiden aiheuttamat seuraukset. Lisäksi työssä esitellään jo markkinoilla olevia älykkäillä ominaisuuksilla varustettuja tietoturvalaitteita, joiden on tarkoitus vastata juuri IoT-laitteiden tietoturvaongelmiin.

Varsinaisena työnä tuotettiin Raspberry Pi alustaa käyttäen samoja tietoturvaominaisuuksia sisältävä sulautettu järjestelmä sekä mobiilisovellus järjestelmän tarkkailuun. Sulautettu järjestelmä sisältää pythonilla kirjoitetun Paketinsuodatuspalomuurin IP-osoitteiden suodatukseen ja estämiseen, sekä REST-palvelimen tiedonvälitykseen Raspberry Pi:n ja mobiilisovelluksen välillä.

Avainsanat: tietoturva, palomuuri, esineiden internet

Tyvelä A, Laakso T. (2019) security problems and solutions of a modern IoT device. University of Oulu, Degree Programme in Computer Science and Engineering. Bachelor's Thesis, 36 p.

ABSTRACT

This bachelor's thesis takes a closer look on the security problems and solutions of a modern IoT device. Thesis covers most common vulnerabilities in IoT design, reasons behind, and consequences that follow. In addition, thesis showcases some of the devices intended specially for IoT security that have already reached the markets.

This thesis also includes design process for a Rasberry Pi based embedded system, that includes same functionality as commercial security devices and a mobile application to monitor the embedded system. System consists of packet-filtering type firewall, written in python, to capture and block unwanted packets and of REST-server to transfer information between firewall and mobile application.

Key words: network security, firewall, internet of things

SISÄLLYSLUETTELO

ALKULAUSE

Tämä työ on tehty osana sulautettujen ohjelmistojen projektia, ja haluamme kiittää Teemu Tokolaa ohjauksesta kurssin aikana.

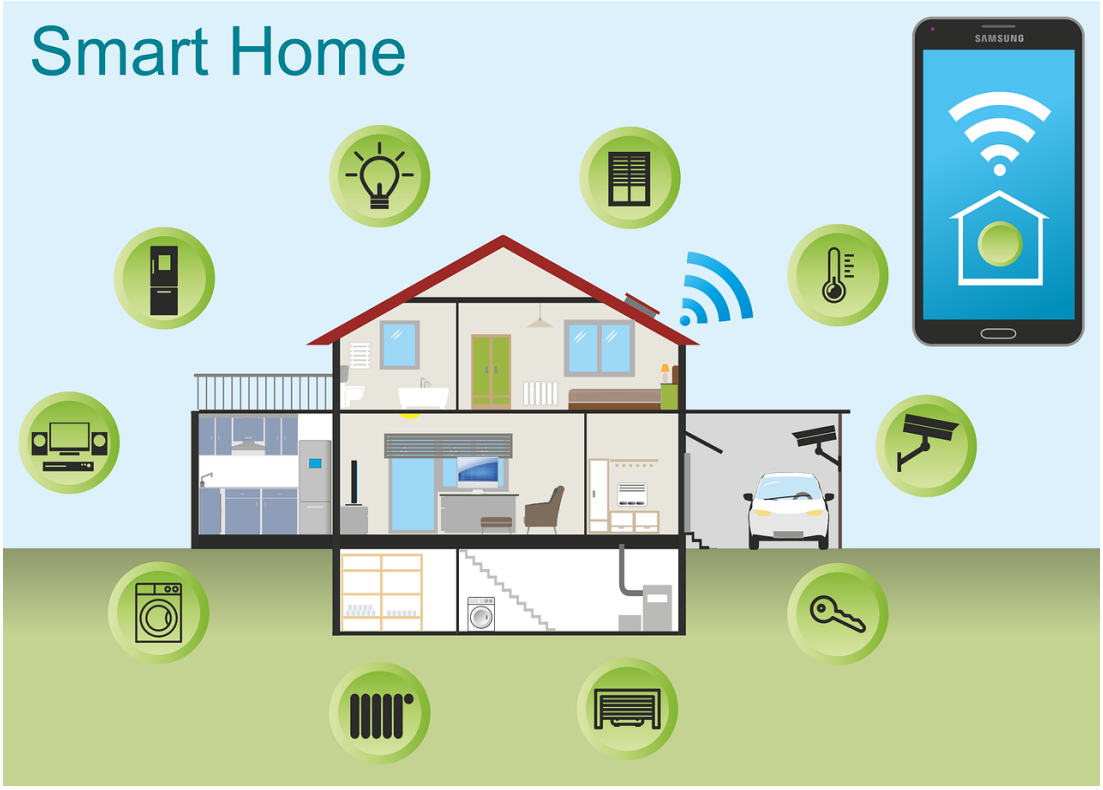
Akseli Tyvelä
Tatu Laakso

LYHENTEIDEN JA MERKKIEN SELITYKSET

API	Application Programming Interface
ARM	Advanced RISC Machine
CPU	Central Processing Unit
DDoS	Distributed-Denial-of-Service
DNS	Domain Name System
DNSBL	Domain Name System Black List
DoS	Denial-of-service
GPU	Graphics Processing Unit
HTTP	Hypertext Transfer Protocol
IoT	Internet of Things
IP	Internet Protocol
JSON	JavaScript Object Notation
LXDE	Lightweight X11 Desktop Environment
RAM	Random-Access Memory
REST	Representational State Transfer
SQL	Structured Query Language
TCP	Transmission Protocol
TOR	Anonymity Network
URL	Uniform Resource Locator
XMR	Monero cryptocurrency

1. JOHDANTO

Teknologian kehittyessä ja komponenttien hintojen laskiessa ovat laitevalmistajat alkaneet lisätä älykkäitä ominaisuuksia yhä useampiin tavallisina pidettyihin kodin laitteisiin. Tietokoneiden ja älypuhelinten lisäksi jääkaapit, itkuhälyttimet ja jopa leivänpaahtimet ovat yhteydessä internettiin. Yhdessä nämä laitteet muodostavat niin sanotun esineiden internetin. Tarkoituksena on tarjota käyttäjille hyödyllisiä sovelluksia, joilla helpottaa kuluttajien elämää. Laitteita voi monitoroida ja ohjata etänä älypuhelimella, jolloin kuluttaja voi esimerkiksi tarkastaa jääkaappinsa sisällön tai ajastaa kahvinkeittimen. Kuvassa 1 on esitettynä yksi näkemys älykkäästä kodista [33].

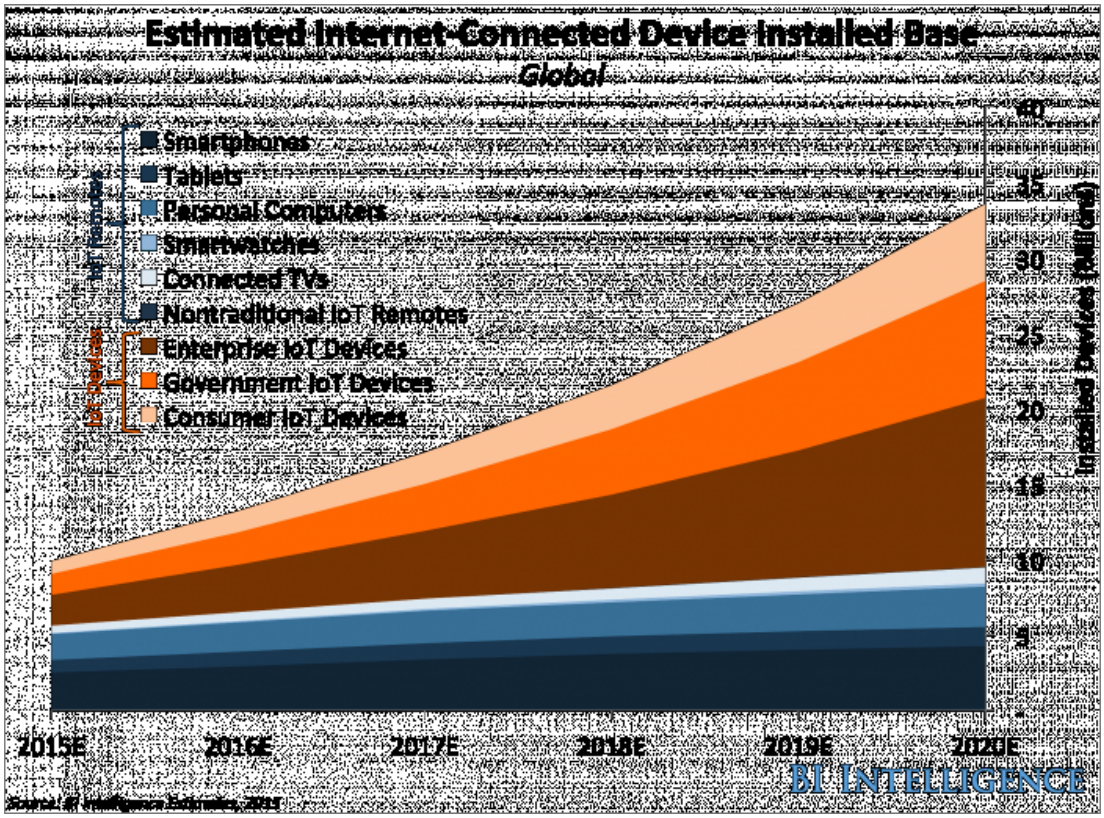


Kuva 1. Esimerkki älykodista.

Näillä arkielämää helpottavilla ominaisuuksilla on kuitenkin varjopuolensa, IoT-laitteiden puutteellinen tietoturva tarjoaa internetissä toimiville rikolliselle ja mahdollisille valtiollisille toimijoille takaportin, jonka kautta laitteet voidaan saada käyttöön omistajansa tietämättä. IoT-laitteista, kuten itkuhälyttimistä, muodostettuja tuhansien laitteiden bottiverkkoja on jo käytetty palvelunestohyökkäyksiin.

Esimerkiksi Mirai-bottiverkko, joka koostui reitittimistä ja IP-kameroista, kaatoi vuonna 2016 useita suosittuja verkkopalveluita kuten Spotifyn, Netflixin ja Twitterin. Bottiverkkojen lisäksi rikolliset toimijat voivat käyttää IoT-laitteiden mikrofoneja sekä kameroita näiden omistajien vakoiluun, mahdollistaen esimerkiksi asuntomurtoja omistajien ollessa pois kotoa.

Vuonna 2009 arvioitu IoT-Laitteiden määrä oli n. 900 miljoonaa ja vuoteen 2020 mennessä laitteiden määrän arvioidaan ylittävän jopa 25 miljardia kappaletta, kuten kuvassa 2 esitetyssä Business Insiderin laatimassa graafissa [34]. Laitteiden lisääntyessä voidaan haittavaikutuksienkin odottaa lisääntyvän. Suurempi laitemäärä mahdollistaa esimerkiksi entistä suuremmat bottiverkot. Siksi IoT-laitteiden tietoturva tulee tulevaisuudessa entistäkin tärkeämmäksi ja markkinoille on jo tuotu laitteita paikkaamaan vajavaista tietoturvaa.



Kuva 2. IoT laitteiden määrän ennustettu kasvu.

IoT-laitteiden tietoturvan parantamiseksi on markkinoille tuotu useita tähän tarkoitukseen suunniteltuja laitteita, mm. Nortonin Core, F-securen Sense ja Cujo AI. Kaikkia laitteita yhdistää korkeahko hinta sekä kuukausimaksullisuus. Kaikkien laitteiden mukana toimitetaan myös mobiilisovellus laitteen ohjaamiseen ja

verkkoliikenteen seurantaan. Tässä työssä esitellään jo markkinoilla olevia tietoturvaratkaisuja. Ja toteutettu vastaavia toiminnallisuuksia sisältävä sulautettu järjestelmä.

2. TAUSTA

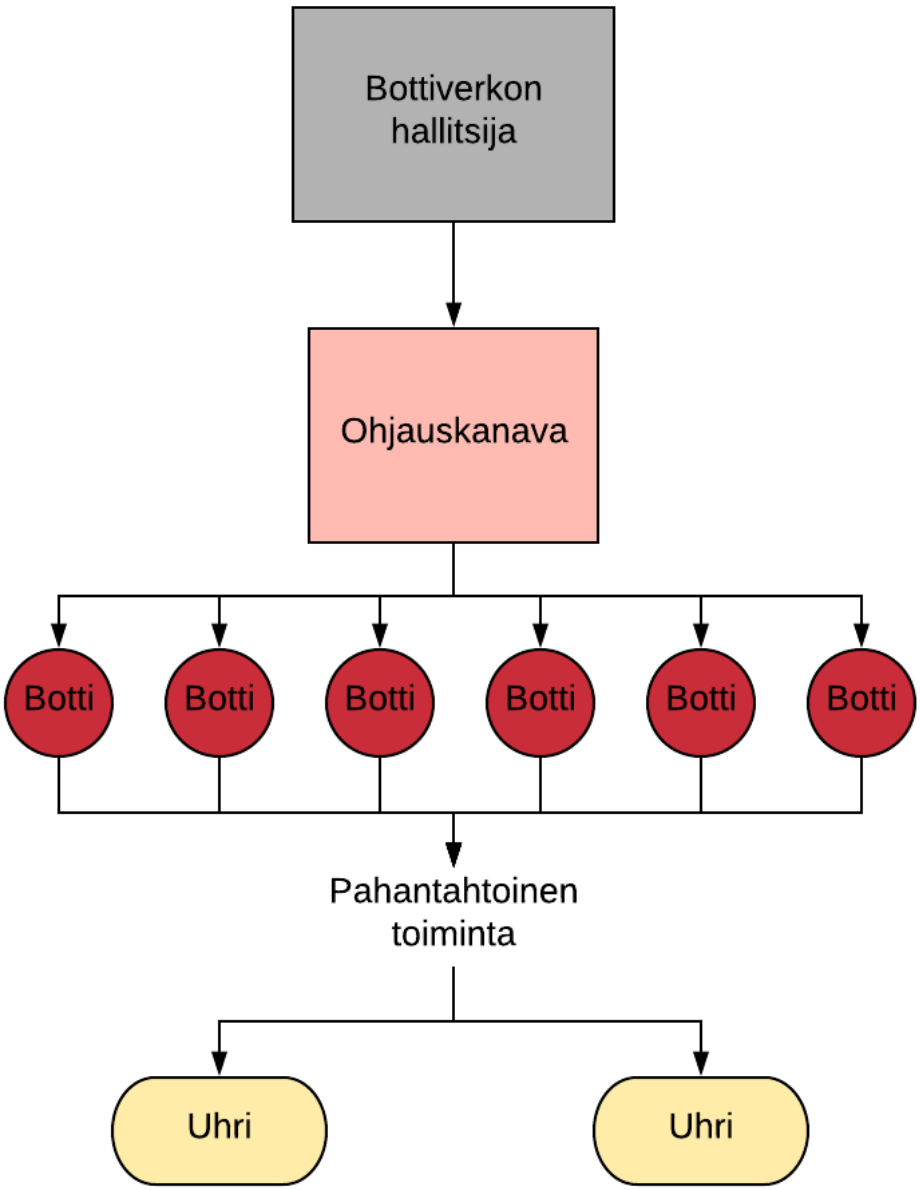
IoT-laitteeksi luokitellaan sellaiset laitteet, jotka sisältävät älykkäitä ominaisuuksia ja joilla on pääsy verkkoon. Kuitenkaan tietokoneita ja mobiililaitteita ei yleensä luokitella IoT-laitteiksi. Vaikka ne osin sopisivatkin määritelmään, ovat ne teknisiltä ominaisuuksiltaan huomattavasti IoT-laitteita kehittyneempiä. IoT-laite on yleensä jokin tavallisena laitteena pidetty kodinkone, kuten jääkaappi, joka sisältää jonkin yksinkertaisen, useimmiten Linux-pohjaisen, sulautetun järjestelmän. IoT-laitteille ominaista on kyky kerätä ja lähettää dataa käyttämällä sulautettuun järjestelmään integroituja sensoreita. Määritelmään sisällytetään usein myös laitteen monitorointi tai ohjattavuus internetin välityksellä. Näiden laitteiden muodostamaa tietoverkkoa kutsutaan esineiden internetiksi.

2.1. Uhat

Suurimman uhan IoT-laitteille muodostaa niiden puutteellinen tietoturva. Laitteiden sisältämät sulautetut piirit ovat yleensä halpoja ja tietoturvan taso on usein puutteellista. On arvioitu, että jopa 70 prosenttia IoT-laitteista sisältävät vakavia aukkoja tietoturvassa [27], jotka eivät ole paikattavissa ohjelmistolla. Nämä aukot mahdollistavat laitteiden kaappauksen ja käyttöönoton erinäisten rikollisten tahojen toimesta. Esimerkiksi eräs Arizonan yliopistossa tehty tutkimus havaitsi, että tutkimuksessa löydetyistä noin 50 000 tulostimesta jopa 20 000 olivat haavoittuvaisia [3].

2.1.1. Bottiverkot

Bottiverkot ovat useista internetiin yhteydessä olevista laitteista koostuvia verkkoja, joiden avulla on mahdollista tuottaa erilaisia verkkohyökkäyksiä. Bottiverkkoihin kuuluvat laitteet ovat useimmiten juuri IoT-laitteita, jotka bottiverkon hallitsija on ottanut käyttöönsä IoT-laitteiden haavoittuvuuksien avulla. Kuvassa 3 kuvataan bottiverkon rakennetta ja toimintaa.

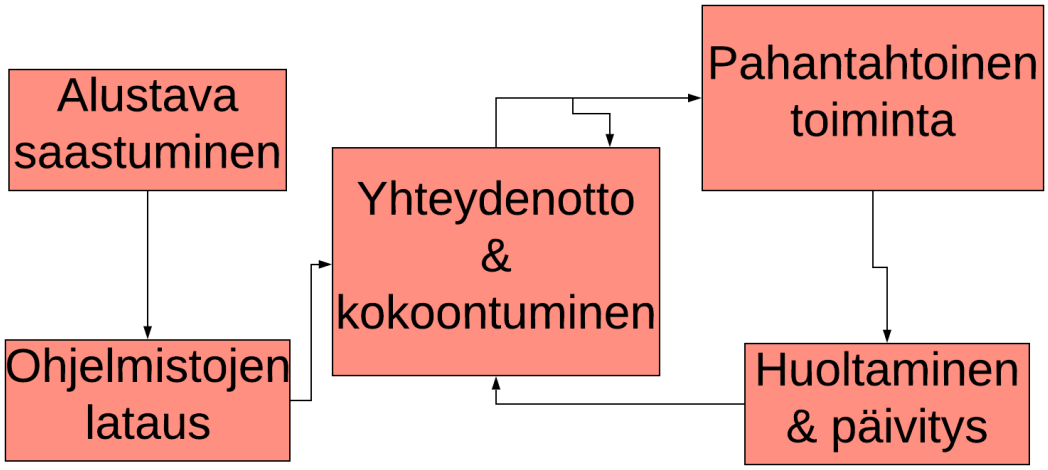


Kuva 3. Bottiverkon rakenne ja toiminta.

Bottiverkon elämänkaari voidaan jakaa viiteen eri vaiheeseen, jotka ovat esitetty kuvassa 4. Ensimmäistä vaihetta sanotaan tarttumisvaiheeksi, jonka aikana laite altistuu virukselle. Viruksen yleisimpiä levitystapoja ovat tiedostojen lataaminen kyseenalaisilta sivuilta, haitallisen sähköpostin liitteen avaaminen, tai verkkosivuilta löytyvien mainosten klikkaaminen. Laite voi myöskin saastuttaa hyödyntämällä laitteesta löytyviä haavoittuvaisuuksia. Asiantuntijat ovat epäilleet, että jopa 25% kaikista internettiin kytketyistä laitteista ovat osana jotakin bottiverkkoa [1]. Tartunnan jälkeen toisessa vaiheessa saastunut laite pakotetaan lataamaan

bottiverkkoa varten suunnitellun ohjelmiston, joka muuntaa laitteen botiksi osana bottiverkkoa. [1][2]

Seuraavassa kokoontumisvaiheessa botti ottaa yhteyden bottiverkon hallitsijan määrittämään johtamis- ja ohjaamiskanavaan (eng. Command & Control channel), joka antaa bottiverkkoon kuuluville boteille käskyjä, jotka ohjaavat sen toimintaa. Tämän jälkeen siirrytään hyökkäämisvaiheeseen, jonka aikana voidaan toteuttaa erilaisia hyökkäyksiä uhreja vastaan. Hyökkäyksen päätteeksi bottiverkko siirtyy ylläpitovaiheeseen, jonka aikana bottiverkon hallitsija kokoaa botit jälleen yhteen bottiverkoksi ja bottiverkko siirtyy takaisin kokoontumisvaiheeseen. Ylläpitovaiheen aikana bottiverkkoa voidaan huoltaa ja päivittää, esimerkiksi tekemällä siitä vaikeammin havaittava viranomaisille. [1][2]



Kuva 4. Bottiverkon elinkaari.

Bottiverkossa olevien laitteiden määrä voi vaihdella tuhansista jopa satoihin tuhansiin laitteisiin. Esimerkiksi avoimen lähdekoodin Mirai-bottiverkko, jota käytettiin useiden suosittujen nettipalvelujen kaatamiseen, kattoi vuonna 2017 noin 380 000 laitetta [36]. IoT-laitteiden määrän kasvaessa, ilman tietoturvan parantamista, voidaan bottiverkkojenkin koon odottaa kasvavan, jolloin rikolliset toimijat saavat käyttöönsä entistäkin suuremmat resurssit.

Bottiverkkoja on myös käytetty kiristämistarkoituksessa. Verkkojen hallitsijat voivat uhata verkkopalveluja tai yrityksiä esimerkiksi palvelunestohyökkäyksillä ja vaatia maksua hyökkäyksen lopettamiseksi tai estämiseksi. Lunnaat vaaditaan useimmiten virtuaalivaluuttana sen tarjoaman anonymiteetin vuoksi.

Bottiverkot eivät ole enää ainoastaan niiden perustajien käsissä, vaan kuka tahansa voi vuokrata bottiverkon käyttöönsä tietyksi ajaksi haluamaansa tarkoitukseen. Bottiverkkojen kauppaa käydään anonyymissa Tor-verkossa erilaisilla foorumeilla ja kauppapaikoilla. Tämä muodostaa yhä suuremman uhan, kun kuka tahansa, teknisesti osaamatonkin, henkilö tai taho voi valjastaa bottiverkon haluamaansa tarkoitukseen.

2.1.2. Vakoilu

IoT-laitteisiin sisällytetyt sulautetut järjestelmät sisältävät usein myös erilaisia sensoreita, kuten kameroita ja mikrofoneja. Tämä yhdistettynä verkkoyhteyteen ja vakaviin tietoturva aukkoihin antaa rikollisille toimijoille mahdollisuuden vakoiluun ja laitteen omistajien tarkkailuun. Myös tietoliikenteen tarkkailu IoT-laitteiden kautta on mahdollista. Laitteiden sensoreilta saatavaa dataa voidaan käyttää rikollisiin tarkoituksiin, kuten kiristykseen arkaluontoisen materiaalin levittämisen uhalla. Vuonna 2015 Fortinet-yrityksen tilastojen mukaan IP-kamerat, sekä reitittimet olivatkin suosituimpia hyökkäyksien kohteita [6].

2.1.3. Kryptovaluutat

Kryptografiaan perustuvien virtuaalisten kryptovaluuttojen syntyminen on herättänyt myös rikollisten toimijoiden kiinnostuksen ja virtuaalisia valuuttoja käytetäänkin laajasti rikolliseen toimintaan niiden anonymiteetin takia. Virtuaalisilla valuutoilla on mahdollista käydä kauppaa anonyymissa Tor-verkossa ja hankkia laittomia tuotteita ja palveluja, kuten huumausaineita.

Kryptovaluutat ovat herättäneet kiinnostusta myös kyberrikollisten keskuudessa ja bottiverkkoja onkin jo valjastettu louhimaan näitä valuuttoja. Kryptovaluuttojen louhinta tarkoittaa käytännössä tietokoneen, yleensä näytönohjaimen, laskentatehon ohjaamista kryptovaluuttojen siirtojen varmistamiseen matemaattisilla yhtälöillä, josta laitteiden omistajat saavat palkkion kryptovaluuttana. Yleensä louhinta vaatii käyttäjältä suurta rahallista panostusta laitteistoon mutta bottiverkkoa hyödyntämällä ei omaa laitteistoa tarvita. Esimerkiksi Smominru-bottiverkkoa, joka on

parhaimmillaan kattanut yli 500 000 laitetta ja tuottanut omistajilleen arviolta kolmen miljoonan dollarin edestä kryptovaluuttaa [28] on käytetty XMR-kryptovaluutan louhimiseen kaapatuilla Windows-palvelimilla. Smominru käytti hyväkseen NSA:n kehittämää ja sittemmin ShadowBrokersin vuotamaa EternalBlue-haavoittuvuutta [29].

Louhinta vaatii kohtuullisen tehokkaan laitteiston ollakseen tuottoisaa. Kuluttajille pelikäyttöön suunnatulla huipputason näytönohjaimella voidaan päästä n. 50 dollarin kuukausituottoon [30]. Koska tuotto on suoraan verrannollinen käytössä olevaan laskenta tehoon, ei yksittäisellä IoT-laitteella saada kummoistakaan tuottoa, mutta bottiverkot sisältävät jopa satojatuhansia laitteita, jolloin päästään jo suurempiin tuottoihin. Avastin suorittamien testien ja laskelmien mukaan 15000 IoT-laitteen muodostama verkko voi tuottaa omistajalleen jopa 1000 dollaria neljässä päivässä [31]. Toisaalta eräs toinen tutkimus totesi, että 50000 laitteen bottiverkolla saataisiin louhittua vain kahden dollarin edestä Litecoin-nimistä kryptovaluuttaa [4]. Louhinnan vaikeustason noustessa myös tuotot pienenevät entisestään.

Suora louhinta ei ole ainoa tapa hyödyntää bottiverkkoja kryptovaluuttojen hankinnassa. Satori-bottiverkkoa on käytetty Claymore -louhintaohjelmiston suojauksen murtamiseen, jolloin bottiverkon omistajat pystyivät vaihtamaan kryptovaluutan siirroissa tarvittavat lompakko-osoitteet omiinsa ja ohjaamaan louhinnan tuottoja omaan lompakkoonsa [32]. Satori on muokattu versio tuhoisasta Mirai-bottiverkosta, mutta potentiaalistaan huolimatta on Satorilla hankittujen tuottojen määrä jäänyt verrattain pieneksi. [7]

2.1.4. DoS/DDoS

Denial of Service Attack, (DoS), eli palvelunestohyökkäys on yleinen ja erittäin haitallinen nettirikollisuuden muoto, jolla pyritään häiritsemään tai kaatamaan internetissä toimivia palveluja, yleensä nettisivuja. Palvelunestohyökkäyksessä hyökkääjä pyrkii internetyhteyden avulla ylikuormittamaan palvelimen resursseja väärillä palvelin kutsuilla. Myös ohjelmistoissa piileviä haavoittuvaisuuksia voidaan pyrkiä hyödyntämään palvelunestohyökkäyksissä.

Distributed Denial of Service, (DDoS), eli hajautettu palvelunestohyökkäys on nimensä mukaan useista lähteistä koostettuja DoS- hyökkäyksiä. DDoS toteutetaan

usein bottiverkkojen avulla, jolloin hyökkäyksen kohteeseen saadaan kohdistettua tuhansien eri laitteiden palvelinkutsuja ja hyökkäyksen volyymi voi olla satoja gigabittejä sekunnissa [13]. DDoS-hyökkäyksiä tapahtuu jatkuvasti ympäri maailmaa. Esimerkiksi joulukuussa 2017 tapahtui yhteensä 610 000 hyökkäystä, joista suurin osa sijaitsi Yhdysvalloissa ja Euroopassa [14]. Vuoden 2018 ensimmäisellä puoliskolla hyökkäysten määrä on laskenut 13% edellisvuoteen verrattuna, hyökkäysten määrän kuitenkin ylittäessä 400 000 joka kuukausi. Huomioitavaa myös on hyökkäysten voimakkuuden olevan samalla nousussa. Helmikuun 28. päivänä GitHub-palvelua kohtaan kohdistetussa hyökkäyksessä dataa liikkui ennätyksellisen 1,3 teratavun sekuntivauhdilla. Tämä ennätys rikottiin vain 5 päivää myöhemmin. Vain kaksi vuotta aiemmin dataa liikutettiin vain 600 gigatavun sekuntivauhdilla [25]. Hyökkäysten voimakkuuden kasvunkin voidaan olettaa noudattavan Mooren lakia, sillä vuonna 2002 suurin voimakkuus oli 100 megatavua sekunnissa [5].

Hyökkäyksiä on hyvin vaikea torjua, sillä yksittäisten lähteiden estäminen ei juurikaan vaikuta tuhansien laitteiden bottinettien toimintaan.

DoS- ja DDoS-hyökkäykset ovat rikollisten suuressa suosiossa, ja niitä käytetään moniin eri tarkoituksiin. DoS-hyökkäykset ovat suosittuja kybervandaalien keskuudessa, jotka ovat usein valmiiksi kirjoitettuja skriptejä käyttäviä nuoria aikuisia. Vandaalit yleensä pyrkivät kaatamaan vaikkapa koulun verkkosivut, tai hakemaan vain huomiota ja adrenaliiniryöppyjä. Vandalismia vakavammat rikokset, kuten kiristys, hyödyntävät puolestaan DDoS-hyökkäyksiä. Kiristäjät uhkaavat yrityksiä hyökkäyksillä, mikäli he eivät maksa vaadittua rahasummaa tai lupaavat lopettaa jo käynnissä olevan hyökkäyksen maksua vastaan. Maksaminen ei kuitenkaan takaa hyökkäyksen loppumista tai sen toteuttamatta jättämistä, rikolliset myös jakavat keskenään informaatiota maksavista yrityksistä, joten maksaminen voi johtaa toistuviin uhkauksiin. Yritykset voivat myös palkata rikollisia tai rahoittaa omia bottiverkkoja, joiden avulla voidaan hyökätä kilpailijoiden verkkoihin. Myös valtiolliset tahot voivat käyttää DDoS-hyökkäyksiä kybersodankäynnissä, jolloin hyökkäysten avulla voidaan kaataa vihollisvaltion infrastruktuuria ja haitata informaatioliikennettä. [15]

2.1.5. Saastuminen

Jotta bottiverkosta saadaan mahdollisimman tehokas, on tarpeen saastuttaa tai kaapata mahdollisimman monta laitetta, yleensä jopa satojatuhansia laitteita. Tietokoneita saastuttaessa tehokas keino on käyttää troijalaisena hevosena tunnettua haittaohjelmaa, joka voi vaikuttaa harmittamattomalta ohjelmalta, mutta suoritettaessa avaa takaportin järjestelmään. IoT-laitteisiin käyttäjät tosin harvemmin asentavat ohjelmistoja Haittaohjelmia levitetään usein sähköpostin liitetiedostona, pop-up-mainoksien avulla sekä tiedostojen latauksen yhteydessä. Laitteen saastumisen havaitseminen on usein hyvinkin hankalaa, sillä ne käyttävät hyvin pienen osan tietokoneen prosessointitehosta, tai ovat horroksessa odottaen bottiverkon omistajan herätettä. Kehittyneemmät ohjelmat voivat jopa aktiivisesti piilotella erilaisilta tietoturvaohjelmistoilta ja skannauksilta, sekä itsenäisesti etsiä haavoittuvaisia laitteita, joiden käyttöjärjestelmät tai tietoturva ovat vanhentuneita [8]. IoT-laitteita ja reitittimiä kaapatessa haittaohjelmat yksinkertaisesti testaavat yleisimpiä käyttäjätunnus-salasana-yhdistelmiä, sillä useat käyttäjät eivät vaivaudu vaihtamaan tehdasasetuksissa valmiiksi määriteltyjä tunnuksia. Eräässä SANS Technology Instituten tekemässä testissä vakioasetuksilla toimivaan kameraan tehtiin 1254 onnistunutta murtautumista noin 46 tunnin aikana [9]. Kehittyneemmät bottiverkot kykenevät murtautumaan laitteisiin käyttämällä niistä löytyviä haavoittuvuuksia, jotka tarjoavat helpon takaoven laitteisiin. Esimerkiksi Reaper niminen haittaohjelma osaa hyväksikäyttää yhdeksää erilaista haavoittuvaisuutta, joita löytyy suurien valmistajien kuten DLinkin valmistamista IP-kameroista [10]. Vuoden 2017 loppusyksystä israelilaisen Check Point-yrityksen mukaan jopa 60 prosenttia sen seuraamista verkoista on Reaperin saastuttamia [11]. Myös kiinalaisen Qihoon mukaan Reaper-bottiberkko on todella laaja ja jopa miljoonia laitteita on jonossa odottamassa bottiverkkoon lisäämistä [12].

2.2. Markkinoilla olevat ratkaisut

IoT-laitteiden mukana tuomat ongelmat on tunnistettu laitevalmistajien toimesta ja markkinoille on tuotu useita tietoturvalaitteita, joiden tarkoitus on verkkoliikenteen suojauksen lisäksi tunnistaa IoT-laitteisiin kohdistuvia uhkia, sekä torjua ne. Seuraavaksi selvitetään kolmen parhaiten tunnetun laitteen ominaisuuksia.

2.2.1. Norton Core

Valmistajan sivut tarjoavat laitteesta hyvin vähän tietoa. Valmistajan mukaan Core kuitenkin hyödyntää tekoälyä ja laitteiden yhdessä muodostamaa tietoverkkoa uhkien tunnistamiseen sekä torjumiseen. Lisäksi Core skannaa jokaisen bitin verkkoon tulevaa dataa mahdollisten uhkien varalta.

Coren 280 dollarin hintaan sisältyy itse laite, mobiilisovellus ja vuoden ohjelmistolisenssi, jonka jälkeen ohjelmiston käyttö maksaa 10 dollaria kuukaudessa. Valmistajan mainostamat kehittyneet ominaisuudet eivät välttämättä ole kuitenkaan korkean hintansa arvoisia. Vaikka Norton Core on kolmesta esitellystä laitteesta kallein, on se jäänyt hienoisesti jälkeen kilpailevista, sekä edullisemmista laitteista kuten F-Secure Sensestä [19]. Saman testin mukaan Core tunnisti 99.4% uhista, kun taas Sense pääsi täyteen 100 prosenttiin [20].

2.2.2. F-secure Sense

Valmistajan mukaan Sense yhdistää perinteisen WiFi – reitittimen sekä tietoturvaohjelmiston ja tarjoaa näin suojaa myös bottiverkkojen ja IoT-laitteiden kaappausten varalta. Uhkien estämiseksi Sense turvaa paikallisen liikenteen skannaukseen ja pilvivalvontaan.

Sensen 199 dollarin hintaan sisältyy itse laite, vuoden lisenssi ohjelmistoon sekä mobiilisovellus, vuoden lisenssin jälkeen ohjelmisto jatkuu samalla 10 dollarin kuukausimaksulla kuin Nortonin Core.

Vaikka Sense käyttää uhkien torjunnassa ainoastaan paikallista liikenteen skannausta, pääsee se samassa Tom´s guiden puolueettomassa testissä [37] parempiin tuloksiin kuin Nortonin Core joka hyödyntää kehittyneempiä teknologioita. Itseasiassa Sense ylsi täyteen 100 prosenttiin. [20]

2.2.3. Bitdefender Box 2

Bitdefender Box eroaa kilpailevista laitteista toimimalla rinnakkain jo olemassa olevan reitittimen kanssa ja pyrkimättä korvaamaan sitä kokonaan kuten Sense Tai Core. Bitdefenderiä voi käyttää myös reitittimenä, mutta valmistajan mukaan se ei kilpaile erillisten reitittimen kanssa.

Bitdefenderin 249 dollarin hinta sisältää laitteen, mobiilisovelluksen sekä vuoden lisenssin tietoturva ohjelmistoon, vuoden jälkeen lisenssi jatkuu 99 dollarin vuosi hintaan. Hinnassa täytyy myös huomioida tarvittava reititin, jolloin hinta voi nousta korkeammaksi kuin Norton Coren.

Tom´s guiden puolueettoman [37] testin mukaan Bitdefender suoriutui testistä 100 prosenttisesti siinä missä F-Securen Sensekin [21].

2.2.4. Suorituskyky

Langattoman verkon suorituskyvyltään laitteista paras on Nortonin Core 672Mbps latausnopeudellaan, Sensen nopeudeksi on mitattu 514Mbps ja Bitdefender jää viimeiseksi 470Mbps:llä. Toki on huomattava, ettei Bitdefenderiä myydä itsenäisenä verkkolaitteena vaan on tarkoitettu toimimaan jo olemassa olevan reitittimen kanssa. Reitittimen kanssa Bitdefender ei juurikaan hidasta verkon latausnopeutta. Ainoastaan latenssi verkkosivuja ladatessa lisääntyi huomattavasti, noin 25 prosentilla. Latausnopeus laski vastaavasti vain noin kuudella prosentilla [20].

Vaikka Bitdefenderiä ei myydä varsinaisena reitittimenä ei se jää juurikaan jälkeen Sensen suorituskyvystä.

Esteitä sisältävässä ympäristössä Bitdefender kuitenkin voittaa noin 30 metrin kantavuudellaan, Coren yltäessä noin 26 metriin ja Sensen jäädessä vain n. 20 metriin. [20] [19] [24]

2.2.5. Tietoturva

Laitteista on vaikea löytää kattavia testejä, varsinkaan tietoturvan osalta. Ainoastaan tomsguide.com on testannut kaikki kolme laitetta. Tietoturvan testaamisen tosin tekee hankalaksi se, että verkko pitää ensin saattaa jollain tapaa hyökkäyksen kohteeksi, jotta tietoturvaa voidaan mitata.

Tomsguiden testeissä kaikkia kolmea laitetta testattiin siirtymällä tunnettuihin haittaohjelmia sisältäviin sivustoihin malwaredomainlist-sivuston kautta. Norton Core torjui yhdeksän kymmenestä [19] vaarallisimmasta sivustosta, F-secure Sense torjui kaikki kymmenen [20] kuten myös Bitdefender Box [21].

Testeissä käytettiin hyväksi myös AV-Test -nimistä tietoturvaohjelmistotestiä. Tom´s guiden mukaan Norton Core suoriutui testistä 99,4 prosenttisesti, Sensen ja bitdefenderin saadessa jälleen 100 prosenttia. Huomioitavaa on myös väärien hälytysten määrä AV-test tietoturvatestin aikana, joita Norton Core antoi 4 kappaletta, Bitdefender vain yhden ja Sense huimat 42 kappaletta. [19]

On myös hyvä huomioida, että esimerkiksi Avira ja Kaspersky Lab-tietoturva ohjelmistot saivat samasta testistä täydet pisteet [23], ilman että tarvitsevat tuekseen kalliin tietoturvareitittimen, ja esimerkiksi Aviran Prime-tietoturvaohjelmiston lisenssi maksaa noin 10 euroa kuukaudessa. Tämä on saman hintainen kuin Coren, Sensen tai Bitdefenderin lisenssit mukana toimitettavan ilmaisen vuoden jälkeen.

Käytännössä laitteiden ainoa etu on juuri IoT-laitteiden turvaamisessa. Tämän testaaminen onkin hankalaa, tai jopa mahdotonta, niihin kohdistuvien hyökkäysten muodon vuoksi, koska yhtä tiettyä kaavaa hyökkäyksille ei ole.

Core luottaa kykyynsä tarkistaa verkkoon tulevat paketit mahdollisesti vaarallisen koodin varalta sekä pyrkii tarkastamaan mahdollisesti vaarallisia käyttäytymismalleja [22].

Sense pyrkii tunnistamaan IoT-laitteisiin liittyviä uhkia tarkistamalla pakettien SNI kentän ja suodattamaan yhteyksiä käyttäen tietoja verkko-osoitteiden aiemmasta toiminnasta. [20].

Parhaimman turvan IoT-laitteille, ainakin paperilla, näyttäisi antavan Bitdefender Box, joka kytketään reitittimen ja internet yhteyden väliin antamaan lisäsuojaa koko verkolle ja kaikille sen laitteille. Box antaa suojaa esimerkiksi SQL-injektioilta, ja tunnistaa poikkeavia käyttäytymismalleja verkkoliikenteestä, jolloin sekatkaisee

liikenteen. Bitdefender Box estää myös ns. brute-force-tunkeutumisen, joka on yleinen tapa murtaa IoT laitteita, sekä sisältää suodattimen lähtevälle liikenteelle, jolloin se voi estää esimerkiksi luottokorttitietoja sisältävän liikenteen. [24]

Kaikki kolme laitetta ovat myös suojattuja WPA2-protokollalla, kuten muutkin yleiset nykyaikaiset langattomat reitittimet.

On hyvä muistaa myös se seikka, että suurinta osaa edellä mainituista ominaisuuksista on vaikea, tai jopa mahdotonta, testata ilman oikeaa hyökkäystä laitetta ja verkkoa kohtaan. Toinen huomioitava asia on myös se, että älykkäät reitittimet ovat jo itsessään IoT-laitteita ja voivat mahdollisesti sisältää haavoittuvuuksia. Vaikka kaikki kolme laitetta ovat WPA2-suojattuja, kuten nykyaikaiset langattomat verkkolaitteet yleensäkin, myös ne ovat murrettavissa helposti saatavilla olevilla ohjelmistoilla, kuten Reaverilla, joka kykenee murtamaan WPA-ja WPA2-salaukset jopa tunneissa [25]. Lisäksi esimerkiksi Mirai-bottiverkko koostui pääosin juuri reitittimistä sekä itkuhälyttimistä.

On siis syytä miettiä, onko kallis tietoturvareititin hienolla designilla rahallisen panostuksen arvoinen, vai onko viisaampaa hankkia vain sellaisia IoT-laitteita, joiden tietoturva on kunnossa jo laitteistotasolla, jolloin kolmannen osapuolen ratkaisuja ei välttämättä tarvita.

3. ALUSTA

Työn tarkoituksena on ollut perehtyä markkinoilla jo tarjolla oleviin IoT- tietoturva ratkaisuihin ja tuottaa samoja toiminnallisuuksia sisältävä sulautettu järjestelmä. Tämän järjestelmän pohjaksi on valittu yhden piirilevyn Raspberry Pi minitietokone, joka sisältää tarvittavat ominaisuudet laitteen toteuttamiseksi.

3.1. Rasberry Pi

Raspberry Pi on hyväntekeväisyysjärjestö Raspberry Pi Foundationin suunnittelema ja markkinoima edullinen yhden piirilevyn minitietokone. Raspberry Pi:stä haluttiin tehdä edullinen ja helppo tapa opettaa sekä lähestyä tietokoneita ja ohjelmointia, laite olikin aluksi tarkoitettu kouluille opetuskäyttöön mutta on sittemmin tuotu kaikkien saataville. [16] Raspberry Pi:stä tulikin nopeasti erittäin suosittu sovellusalusta ja ensimmäinen yleiseen myyntiin tuotu 10000 kappaleen erä Raspberry Pi Model B:tä myytiin loppuun minuuteissa [17]. Sittemmin Raspberry Pi:stä on tuotu markkinoille kahdeksaa eri versiota, joita on myyty yhteensä yli 12 miljoonaa kappaletta vuoden 2012 julkaisun jälkeen [18].

3.2. Rasberry Pi 2 Vs. 3

Työtä varten yliopisto tarjosi Raspberry Pi 2 Model B minitietokoneen, joka on Pi:n toinen kehitysversio, vaikka Pi 2 tarjoaakin riittävät ominaisuudet laitteet toteuttamiseksi, huomattiin heti projektin alussa merkittäviä yhteensopivuusongelmia Pi:n ja reitittimen välillä. Raspberry Pi 2:n tilalle hankittiin Raspberry Pi 3 Model B sekä Asus RT-N12+ reititin yhteensopivuusongelmien minimoimiseksi. Raspberry Pi:n kahden eri version eroavaisuudet selviävät taulukosta 1 [35].

Taulukko 1. Rasberry Pi:n ominaisuuksista.

	Raspberry Pi 3 Model B	Raspberry Pi 2 Model B
Introduction Date	2/29/2016	2/2/2015
SoC	BCM2837	BCM2836
CPU	Quad Cortex A53 @ 1.2GHz	Quad Cortex A7 @ 900MHz
Instruction set	ARMv8-A	ARMv7-A
GPU	400MHz VideoCore IV	250MHz VideoCore IV
RAM	1GB SDRAM	1GB SDRAM
Storage	micro-SD	micro-SD
Ethernet	10/100	10/100
Wireless	802.11n / Bluetooth 4.0	none
Video Output	HDMI / Composite	HDMI / Composite
Audio Output	HDMI / Headphone	HDMI / Headphone
GPIO	40	40
Price	$35	$35

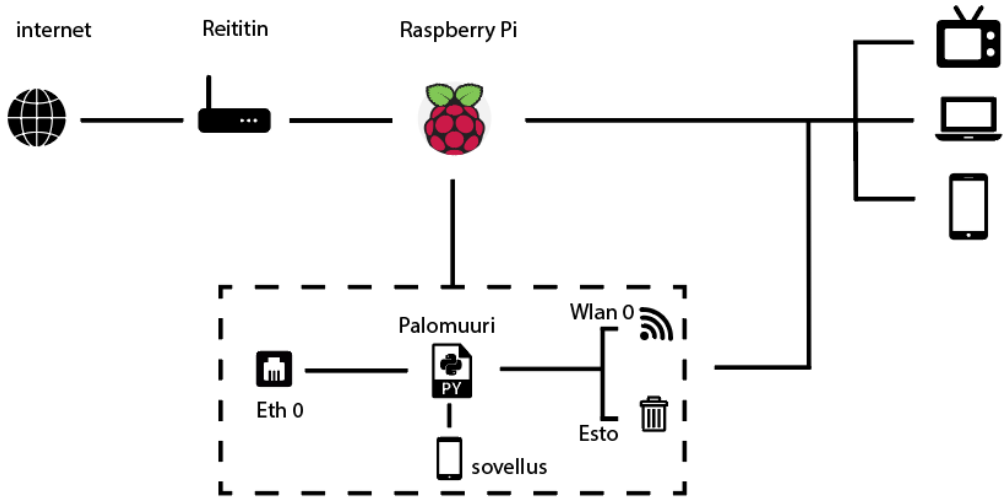
Suurimpana erona Pi 3 tarjoaa huomattavasti tehokkaamman suorittimen sekä grafiikkaohjaimen. Pi 3:een on myös integroitu langaton verkkokortti, joka mahdollistaa Pi:n käytön langattoman verkon tukipisteenä ilman erillistä WiFi-sovitinta toisin kuin Pi 2.

3.3. Konfiguraatio

Järjestelmäämme varten Pi:hin on asennettu Raspbian-käyttöjärjestelmä, joka on Debian pohjainen, Raspberry Pi:n kevyelle ARM suorittimelle optimoitu Linux jakelu, josta valitsimme graafisen työpöytäympäristön sisältävän version, joka on niin ikään Raspberry Pi:lle optimoitu versio LXDE-työpöytäympäristöstä.

Raspbiania jaellaan myös komentoriviversiona, ilman graafista työpöytää, mutta se ei tarjoa käytännön tehonlisäystä, joten valitsimme testauksen helpottamiseksi graafisen vaihtoehdon.

Työn kannalta oli oleellista, että oma laitteemme, markkinoilla olevien laitteiden tapaan, toimii myös langattoman verkon tukipisteenä. Käytännössä tämä tapahtui siltaamalla Pi:n langallisen ja langattoman verkon sovittimet, wlan0 ja eth0, yhdeksi verkoksi, jolloin kaikki wlan sovittimeen liitettyjen laitteiden liikenne ohjautuu ethernet portin läpi. Tämä myös edesauttaa myöhemmässä vaiheessa liikenteen kaappaamisessa ja suodattamisessa, kun tarkastelun kohteena on vain yksi liittymä. Kuvassa 6 on kuvattuna järjestelmän toiminta.



Kuva 6. Kaavio järjestelmän toiminnasta

4. PALOMUURI

Oleellisinta laitteen toiminnassa on jonkinlainen palomuuri verkkoliikenteen suodattamiseksi, jonka toteuttamiseen on monia vaihtoehtoja. Tässä työssä päädyttiin ns. Packet Filtering -ratkaisuun, jossa haitallinen liikenne suodatetaan yksittäisten IP-pakettien perusteella, ja tässä tapauksessa pakettien sisältämän IP-osoitteen perusteella. Tällä menetelmällä saadaan haitallinen liikenne karsittua suhteellisen helposti ja tehokkaasti, kunhan tiedossa olevien haitallisten osoitteiden määrä on tarpeeksi suuri ja lähde luotettava.

4.1. Pakettien kaappaus

Pakettien kaappaamiseksi suodatusta varten käytettiin työssä hyväksi TShark-analysaattoriohjelmaa, joka on terminaaliversio suositusta Wireshark-pakettianalysaattorista joka mahdollistaa verkkoliikenteen kaappaamisen, tallentamisen ja analysoinnin. Tshark valittiin sille suunnitellun pyshark wrapper -laajennuksen takia. Kyseisen laajennuksen avulla kaapatut paketit voidaan tuoda python kieliseen ohjelmaan ja niitä voidaan käsitellä ohjelman sisällä lähes reaaliajassa Tsharkin tarjoamien työkalujen sekä itse kirjoitetun ohjelman avulla.

Pyshark mahdollistaa liikenteen kaappauksen halutusta liittymästä halutulla aikajaksolla sekä sen tallentamisen muuttujiin tai tiedostoon. Tässä tapauksessa paketit kaapataan eth0-liittymästä, kaiken liikenteen kulkiessa sen kautta, käyttämällä LiveCapturen Continiously-ominaisuutta, jolla ohjelma kaappaa kaikki paketit ohjelman käynnistämisestä sen lopettamiseen. Tämän jälkeen paketit tallennetaan muuttujaan suodatusta varten.

4.2. Pakettien suodatus

Kuten mainittu, paketit päätettiin suodattaa niiden sisältämän IP-osoitteen perusteella, jolloin pakettien hyvyys on helposti ja konkreettisesti määritettävissä vertaamalla sitä haitallisiin IP-osoitteisiin ja määrittämällä numeerinen kynnysarvo sille, montako haitallista hakutulosta IP-osoitteelle sallitaan ennen paketin hylkäämistä

Kaapattuja paketteja iteroidaan niiden saapumisjärjestyksessä. Ensimmäisenä paketeista hylätään ne, jotka eivät sisällä IP-kerrosta, ja täten eivät IP-osoitettakaan, näiden pakettien IP-osoitteeksi ohjelma määrittää ”noip”, jolloin ne hylätään seuraavassa vaiheessa. Jos paketti sisältää IP-kerroksen, tallennetaan paketin IP-osoite muuttujaan.

Toisessa vaiheessa IP-osoitetta verrataan erilaisiin IP-osoite listauksiin, joita on kolmenlaisia:

1. Ohjelman sisäiset listaukset,
2. URL-listaukset ja
3. DNSBL-listaukset.

Ohjelman sisäisiin listauksiin kuuluvat Default, Safe- ja Blocked-listat. Default-lista sisältää esimerkiksi verkon reitittimen IP-osoitteen, jolla vältytään tarpeettomilta tarkastuksilta. Safe- ja Blocked-listat taas sisältävä jo läpikäydyt IP-osoitteet, jotka on luokiteltu joko turvallisiksi tai haitallisiksi osoitteiksi. Vaikka osoitteen luokittaminen turvalliseksi ei ole pitkällä tähtäimellä luotettavaa tai turvallista, näin säästetään kuitenkin huomattavasti resursseja, jotka ovat Raspberry Pi:n tapauksessa rajalliset.

URL-listaukset sisältävät eri tahojen ylläpitämiä html muotoisia tekstitiedostoja mahdollisesti eri tavalla haitallisista IP-osoitteista, esimerkiksi torstatus.blutmagie.de listaa mahdollisia TOR-verkon poistumiskohtia ja emergingthreats.net puolestaan listaa muun muassa eri tahoilta saamiaan osoitteita spamboteista, Zeus-bottiverkosta sekä pitää ”top-listaa” verkkohyökkääjistä.

URL-listauksia tarkistettaessa ohjelma yksinkertaisesti avaa URL-soitteen tekstitiedoston ja vertaa onko tarkastelun kohteena oleva IP-osoite listalla ja palauttaa totuusarvon TRUE/FALSE.

DNSBL on lyhenne sanoista ”Domain Name System Blacklists”, joka perustuu internetin nimipalvelujärjestelmään (DNS). Nimipalvelujärjestelmän avulla voidaan suorittaa kysely nimipalvelimelle (eng. Resolver) siitä, tunteeko se kysyttävän IP-osoitteen. DNSBL:n tapauksessa nimipalvelin vastaa, onko kysytty IP-osoite haitallinen vai ei. Useimmat DNSBL-palvelut listaavat lähinnä sähköpostille haitallisia spambotteja, mutta joukosta löytyy myös esimerkiksi bottiverkkoja seuraavia DNSBL-listauksia.

Oleellista on suorittaa IP-osoitteen vertailu listoihin edellä mainitussa järjestyksessä resurssien säästämiseksi. Nopeinta on tarkastaa IP-osoitteita ohjelman sisäisiin listoihin verrattuna, DNSBL-palvelun ollessa hitain ja yhteydeltään epävarmin.

Jokaisen IP-osoitteen mukana kuljetetaan muuttujaa BAD, joka on iteraation alussa 0 ja johon voidaan jokaisen lista osuman jälkeen lisätä 1. Näin palomuurin seulaa voidaan säätää tiukemmaksi tai väljemmäksi niin haluttaessa. Kuitenkin resurssien säästämiseksi palomuuri estää IP-osoitteen heti sen saadessa haitallisen osuman joltain listalta, jolloin jokaiselle IP-osoitteelle ei tarvitse tehdä URL- ja DNSBL- kyselyä, jotka vievät huomattavasti aikaa riippuen kyseltävien URL-osoitteiden ja DNSBL-palveluiden määrästä. Raspberry Pi:n rajallinen laskentateho rajoittaa huomattavasti palveluiden määrää, toisaalta parhaimmassa tapauksessa haitallinen osoite voidaan estää jo yhden URL-kyselyn jälkeen.

4.3. Pakettien estäminen

Pakettien estämisessä käytettiin linux-kerneliin sisäänrakennettua iptables-suodatinta, johon voidaan komentoriviltä kirjoittaa erilaisia palomuurisääntöjä liikenteen ohjaamiseksi tai estämiseksi. Käytännössä ohjelma sisältää funktion, jota kutsutaan tietyn BAD-muuttujan raja-arvon ylittyessä, joka avaa taustalle uuden prosessin, jossa komentoriville kirjoitetaan kaavassa 1 esitetty ennalta määritetty komento IP-osoitteen estämiseksi.

"sudo /sbin/iptables -A INPUT -s "+ packet_ip +" -j DROP" (1)

5. MOBIILISOVELLUS

Työssä oli myös oleellista tuottaa mobiilisovellus sillä myös jo markkinoilla olevat tietoturvaratkaisut sisältävät usein mobiilisovelluksen liikenteen tarkkailuun ja laitteen ohjaamiseen.

Mobiilisovelluksen kehittämisessä käytettiin Unity3D-pelinkehitysympäristöä sen tukiessa useita eri alustoja mm. androidia sekä C#-ohjelmointikieltä. Vaikka Unity onkin lähinnä 3D-pelimoottori, se sisältää myös kattavat työkalut graafisen käyttöliittymän nopeaan luomiseen ilman suurta määrää ohjelmointia. Lisäksi käytettävissä oleva C# -kieli sisältää Microsoftin .NET kirjastot joka mahdollistaa http-yhteyden REST serverin ja sovelluksen välillä tiedonsiirtoa varten.

Käytännössä sovellus sisältää funktiot, joilla haetaan tietyn ajan välein REST-palvelimelta tiedot haitallisten pakettien sekä pakettien kokonaismäärästä ja ne esitetään käyttäjälle graafisessa muodossa.

6. REST-PALVELIN

Palomuurin ja mobiilisovelluksen välinen tiedonsiirto hoidetaan REST-API:n avulla, joka pohjautuu HTTP -protokollaan. API:in voidaan kirjoittaa ja sieltä voidaan hakea tietoja päätepisteiden avulla, jotka ovat käytännössä URL-osoitteita, jotka ohjaavat oikeaan resurssiin. Resurssit ilmaistaan usein JSON-formaatissa, joka on ominaista REST-API:lle.

Käytettävä REST-API sisältää yhden REST-palvelimen sekä kaksi asiakasohjelmaa. Palvelinta suoritetaan Raspberry PI:llä erillisenä ohjelmana ja palomuuri sekä mobiilisovellus sisältävät kumpikin yhden asiakasohjelman. Käytännössä palomuuri pitää kirjaa haitallisten pakettien ja pakettien kokonaismääristä, jotka se ilmoittaa jokaisella iteraatiolla palvelimelle, jossa tiedot kirjoitetaan JSON muodossa talteen tiettyihin resursseihin. Mobiilisovellus taas hakee samat tiedot aina 10 sekunnin välein, jotta tiedot kuitenkin ovat suhteellisen reaaliaikaisia ja palvelinkuorma pysyy maltillisena.

Serveriä suoritetaan ns. paikallista osoitetta ”http://0.0.0.0:5000” käyttäen, johon asiakasohjelmat ottavat yhteyden. Tiettyyn resurssiin voidaan osoittaa URL-osoitteella ”http://0.0.0.0:5000/resursin_nimi/”. Esimerkiksi haitallisten pakettien määrään voidaan osoittaa osoitteella ” http://0.0.0.0:5000/badpkts/”. Jokaista osoitetta varten määrätään halutut http-kutsut, joilla suoritetaan tiettyjä toimenpiteitä. Esimerkiksi /badpkts/-resurssi sisältää kutsut GET ja POST, joka http GET-kutsulla palauttaa mobiilisovellukselle pakettien määrän, ja kutsulla POST taas tallentaa palomuurin lähettämän pakettien määrän.

Näin tiedonsiirto voidaan suorittaa sen vaikuttamatta palomuurin tai mobiilisovelluksen toimintaan ja päinvastoin, tällöin esimerkiksi sovelluksen vikatilanteessa palomuuri toimii edelleen normaalisti.

Koska palvelinta suoritetaan paikallisesta osoitteesta, jota ei tietoturvasyistä ole avattu internettiin päin, voi REST-palvelinta kutsua ainoastaan saman verkon sisästä. Tällöin myös http-kutsun onnistumiseksi täytyy puhelimen tai muun laitteen olla samassa verkossa kuin Raspberry PI:n.

7. JATKOKEHITYS

Vaikka tässä työssä tuotettu sulautettu järjestelmä toimii tietoturvalaitteena vähintään konseptitasolla, ja sisältää näennäisesti samoja toiminnallisuuksia kuin markkinoilla olevat ratkaisut, sisältää järjestelmä kuitenkin tiettyjä puutteita. Nämä olisi korjattava laitteen jatkokehitystä sekä kaupallistamista silmällä pitäen. Näitä ovat:

1. Laitteen suorituskyky,
2. Ohjelmiston suorituskyky,
3. Mobiilisovelluksen ominaisuudet ja
4. IP-listausten määrä ja luotettavuus.

Kuten jo aiemmin mainittu, on järjestelmän pohjana käytetyn Raspberry Pi:n suorituskyky suhteellisen rajallinen sekä laskentatehonsa että langattoman verkkokortin nopeuden puolesta. Langattoman verkon nopeus jäi auttamattoman hitaaksi 30Mbps nopeudellaan, joka on reitittimen nopeudeksi liian hidas, jotta Pi:tä voitaisiin käyttää reitittimenä.

Laskentatehon puute ilmenee palomuurin toiminnan hidastumisena IP-osoitteita käsitellessä, yhden IP-osoitteen käsittelyyn voi kulua jopa useita sekunteja, jos ohjelma joutuu käymään läpi useita URL- tai DNSBL-listauksia ja ongelma eskaloituu entisestään, jos verkossa on samanaikaisesti paljon liikennettä ja REST-serveriä suoritetaan yhtä aikaa.

Pi:n laitetason puutteellista suorituskykyä voitaisiin paikata ainakin osittain ohjelmiston optimoinnilla, esimerkiksi kirjoittamalla palomuuri käyttämään useampaa säiettä IP-osoitteiden käsittelyyn, jolloin voitaisiin käsitellä useampaa IP-osoitetta yhtä aikaa. Lisäksi koodin refaktoroinnilla, eli uudelleen järjestämisellä, voitaisiin koodista poistaa sitä mahdollisesti hidastavia silmukka ja ehtorakenteita. Kaupallisen tuotteen osalta järkevin ratkaisu olisi toteuttaa laskenta jossain muualla kuin itse palomuurin sisältävällä laitteella, esimerkiksi palvelinpohjaisesti.

Mobiilisovellus sellaisenaan ei täytä nykyisiä standardeja toiminnallisuuden eikä käyttöliittymän osalta. Jo markkinoilla olevien tietoturvalaitteiden mukana toimitettavat sovellukset sisältävät enemmän ominaisuuksia laitteen tilan tarkkailuun ja ohjaamiseen. Tätä työtä varten tuotettu mobiilisovellus esittää ainoastaan hyvien sekä hylättyjen pakettien määrät, joten käyttäjälle esitettävän informaation määrää tulisi lisätä kattamaan esimerkiksi verkossa oleviin laitteisiin, sekä antamaan

käyttäjälle dataa verkon käytöstä esimerkiksi graafin muodossa. Lisäksi olennaista olisi lisätä käyttäjälle tarpeellisia työkaluja laitteen hallintaan.

Tällä hetkellä järjestelmä tarkastaa IP-osoitteita kahden URL-listan ja kuuden DNSBL-listauksen perusteella, ja vaikka nämä listat kattavat yhteensä tuhansia IP-osoitteita, on määrä silti liian alhainen, jotta palomuuri voisi toimia luotettavasti. Suuremman tietokannan mukana myös lähteiden luotettavuus kasvaisi, useita listauksia tarkastellessa kynnysarvoa IP-osoitteen hylkäämiseksi voitaisiin nostaa yhdestä ylöspäin ja vaatia että IP-osoite löytyisi esimerkiksi kolmelta listalta ennen sen hylkäämistä. Tällöin mahdollisesti vääristä syistä listalle joutuneet osoitteita ei välttämättä hylättäisi. Lisäksi eri listauksia voisi arvottaa tietyin perustein niiden luotettavuuden mukaan.

Suuremman tietokannan saavuttamiseksi on järjestelmän suorituskyvyn kuitenkin kasvettava huomattavasti, sillä esimerkiksi DNSBL.info listaa 57 kappaletta DNSBL-listoja, joista ohjelma tällä hetkellä käsittelee kuutta, joiden lisäksi URL-listauksia on tarjolla eri tahoilta lähes loputon määrä.

8. AJANKÄYTTÖ

Suurin osa työtunneista käytettiin yhteisissä tapaamisissa. Tapaamisten aikana etsittiin aiheeseen liittyvää tietoa, esitettiin ideoita ja tehtiin kirjoitustyötä. Tapaamisten lisäksi molemmat tekivät tahoillaan työtä, lähinnä kirjoittamista ja ohjelmointia, myös itsenäisesti, joka koottiin tapaamisissa yhteen. Taulukossa 1. esitettynä työhön käytetyt tuntimäärät.

Nimi	Tunnit
Akseli Tyvelä	247
Tatu Laakso	253

Taulukko 2. Työhön käytetyt tunnit.

9. YHTEENVETO

IoT-laitteiden määrän kasvaessa joka vuosi on laitteiden puutteellinen tietoturva muodostumassa yhä suuremmaksi ongelmaksi. Yksi suurimmista ongelmista on IoT-laitteista koostuvien bottiverkkojen avulla suoritetut hyökkäykset, joiden määrä sekä hyökkäysten voimakkuus ovat kasvussa IoT-laitteiden lisääntyessä. Puutteet laitteiden tietoturvassa ovat johtaneet uuden tuotekategorian syntyyn ja markkinoille on tuotu useita kolmannen osapuolen tietoturvaratkaisuja suunnattuna erityisesti IoT-laitteille.

Tässä työssä keskityttiin IoT-laitteiden tietoturvaongelmiin yleisellä tasolla sekä esiteltiin markkinoilla tarjolla olevia kolmannen osapuolen ratkaisuja. Lisäksi työssä tuotettiin vastaavia ominaisuuksia sisältävä sulautettu järjestelmä.

Sulautetun järjestelmän avulla pyrittiin tunnistamaan ja estämään tietoliikenne mahdollisesti haitalliseen IP-osoitteeseen kaappaamalla kaikki verkkoon tulevat IP-paketit ja vertaamalla paketin sisältämää IP-osoitetta erilaisiin listoihin haitallisiksi tiedetyistä IP-osoitteista.

Toimiessaan oikein järjestelmä tunnisti haitallisia IP-osoitteita ja onnistui estämään ne kirjoittamalla uusia sääntöjä Linuxiin integroituun iptables-suodattimeen. Ongelmaksi muodostuivat ne paketit, jotka sisälsivät IPv6-protokollan mukaisen heksadesimaaleina esitetyn IP-osoitteen, ohjelman tunnistaessa, ja listojen tarjotessa, IPv4-protokollan mukaisia desimaaleina esitettyjä IP-osoitteita. IPv6-protokollan mukaiset IP-osoitteet jätettiin käsittelemättä. Lisäksi ongelmia aiheuttivat paketit, jotka eivät sisältäneet IP-kerrosta, josta käsiteltävä IP-osoite haettiin.

Ohjelman testaamiseksi käytettiin TCP/IP-protokollan ping-työkalua, joka kokeilee määrätyn IP-osoitteen saavutettavuutta. Haitalliksi tiedettyä IP-osoitetta pingatessa järjestelmä tunnisti haitalliset osoitteet ja katkaisi yhteyden. Lisäksi pidemmän, noin kuuden tunnin testijakson aikana laite tunnisti ja esti kaksi kappaletta verkkoon itsenäisesti yhteyden ottanutta IP-osoitetta.

10. LÄHTEET

[1] S. C. Silva, Sergio & M. P. Silva, Rodrigo & Pinto, Raquel & M. Salles, Ronaldo. (2013). Botnets: A survey. Computer Networks. 57. 378–403. 10.1016/j.comnet.2012.07.021.

[2] Karim, Ahmad & Salleh, Rosli & Shiraz, Muhammad & Shah, Syed & AWAN, Irfan & Anuar, Nor. (2014). Botnet detection techniques: review, future trends and issues. 15. 10.1631/jzus.C1300242.

[3] M. Patton, E. Gross, R. Chinn, S. Forbis, L. Walker and H. Chen, "Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT)," 2014 IEEE Joint Intelligence and Security Informatics Conference, The Hague, 2014, s. 232-235.

[4] Jan-Willem Nijhuis (2017) Effect of IoT botnets on Cryptocurrency. University of Twente.

[5] Kishore Angrishi (2017) Turning Internet of Things(IoT) into Internet of Vulnerabilities.

[6] Victor Larsson (2017) IoT – an internet of threats? Identifying the dangers of an IoT-instance. Faculty of Computing, Blekinge Institute of Technology

[7] Dan Goodin (17.1.2018) New botnet infects cryptocurrency mining computers, replaces wallet address
URL: https://arstechnica.com/information-technology/2018/01/in-the-wild-malware-preys-on-computers-dedicated-to-mining-cryptocurrency/

[8] Panda Security mobile news (5.12.2017) What is a botnet
URL: https://www.pandasecurity.com/mediacenter/security/what-is-a-botnet/

[9] Ionut Ilascu (12.9.2017) Bots Infect Insecure IoT Device Every Two Minutes
URL: https://www.bitdefender.com/box/blog/iot-news/bots-infect-insecure-iot-device-every-two-minutes/

[10] 360 Netlab Blog (20.10.2017) IoT_reaper: A Rappid Spreading New IoT Botnet
URL: http://blog.netlab.360.com/iot_reaper-a-rappid-spreading-new-iot-botnet-en/

[11] Check Point Research (19.10.2017) A New IoT Botnet Storm is Coming
URL: https://research.checkpoint.com/new-iot-botnet-storm-coming/

[12] Andy Greenberg (20.10.2017) The Reaper IoT Botnet Has Already Infected a Million Networks

URL: https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/

[13] Sean Michael Kerner (29.1.2018) Peak DDoS Attack Volume Declines to 600G bps in 2017, Arbor Reports
URL: http://www.eweek.com/security/peak-ddos-attack-volume-declines-to-600g-bps-in-2017-arbor-reports

[14] Arbor Network ATLAS (12.2017)
URL: http://resources.arbornetworks.com/wp-content/uploads/ATLAS-Global-12.2017.pdf

[15] Imperva Incapsula Distributed Denial of Service (DDoS)
URL: https://www.incapsula.com/ddos/denial-of-service.html

[16] Eric Escobar (7.3.2013) What Is the Raspberry Pi?
URL: https://www.quickanddirtytips.com/tech/computers/what-is-the-raspberry-pi

[17] Kevin Parrish (29.2.2012) $35 Raspberry Pi Model B Sold Out Within Minutes
URL: https://www.tomshardware.com/news/Raspberry-Pi-Eben-Upton-RS-Components-Premier-Farnell-Linux,14851.html

[18] Paul Miller (17.2.2017) Raspberry Pi sold over 12.5 million boards in five years
URL: https://www.theverge.com/circuitbreaker/2017/3/17/14962170/raspberry-pi-sales-12-5-million-five-years-beats-commodore-64

[19] Brian Nadel (6.11.2017) Norton Core Router Review
URL: https://www.tomsguide.com/us/norton-core-router,review-4827.html

[20] Brian Nadel (1.11.2017) F-Secure Sense Review
URL: https://www.tomsguide.com/us/f-secure-sense,review-4801.html

[21] Brian Nadel (10.11.2018) Bitdefender 2019 Review: Superior Protection, Low Performance Impact
URL: https://www.tomsguide.com/us/bitdefender,review-3983.html

[22] Brian Nadel (6.11.2017) Norton Core Router Review
URL: https://www.tomsguide.com/us/norton-core-router,review-4827.html

[23] Bogdan Popa (24.5.2017) The Best Windows 10 Antivirus of 2017
URL: http://news.softpedia.com/news/the-best-windows-10-antivirus-of-2017-515985.shtml

[24] Brian Nadel (11.11.2018) Bitdefender Box (2018) Review: Flexible Protection
URL: https://www.tomsguide.com/us/bitdefender-box,review-3766.html

[25] Adam Pash (9.1.2012) How to Crack a Wi-Fi Network's WPA Password with Reaver
URL: https://lifehacker.com/5873407/how-to-crack-a-wi-fi-networks-wpa-password-with-reaver

[26] Calyptix (10.8.2018) DDoS Attacks 2018: New Records and Trends
URL: https://www.calyptix.com/top-threats/ddos-attacks-2018-new-records-and-trends/

[27] HP News (29.7.2014) HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack.
URL: https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676

[28] Danny Palmer (1.2.2018) A giant botnet is forcing Windows servers to mine cryptocurrency.
URL:http://www.zdnet.com/article/a-giant-botnet-is-forcing-windows-servers-to-mine-crytocurrency/

[29] Zack Whittaker (14.4.2017) NSA's arsenal of Windows hacking tools has leaked.
URL:http://www.zdnet.com/article/shadow-brokers-latest-file-drop-shows-nsa-targeted-windows-pcs-banks/

[30] Profitability calculator.
URL: https://www.nicehash.com/profitability-calculator

[31] Arjun Kharpal (1.3.2018) 15,000 internet-connected devices could be hacked to mine $1,000 of cryptocurrency in 4 days.
URL:https://www.cnbc.com/2018/03/01/thousands-of-iot-devices-can-be-hacked-to-mine-cryptocurrency-avast.html

[32] 360 Netlab Blog (17.1.2018) Art of Steal: Satori Variant is Robbing ETH BitCoin by Replacing Wallet Address.
URL:http://blog.netlab.360.com/art-of-steal-satori-variant-is-robbing-eth-bitcoin-by-replacing-wallet-address-en/

[33] URL: http://reporterexpert.com/wp-content/uploads/2017/08/jason-hope-smart-home.png

[34] URL:
https://static2.businessinsider.com/image/563d14a69dd7cc18008c818a-700-517/unnamed.png

[35] URL: https://hackadaycom.files.wordpress.com/2016/02/pispecs2.png

[36] McAfee Labs 4/2017 McAfee Labs Threats Report.
URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2017.pdf

[37] Tom´s guide 14.8.2018 About Tom´s guide.
URL: https://www.tomsguide.com/us/toms-guide-who-we-are,review-4166.html